

# Kummer Spaces in Cyclic Algebras of Prime Degree

Adam Chapman

*Department of Mathematics, Michigan State University, East Lansing, MI 48824*

David J. Gryniewicz

*University of Memphis, Department of Mathematical Sciences, Memphis, TN 38152, USA*

Eliyahu Matzri

*Department of Mathematics, Ben-Gurion University, Beer-Sheva, Israel*

Louis H. Rowen, Uzi Vishne

*Department of Mathematics, Bar-Ilan University, ramat-gan 5290002, Israel*

---

## Abstract

We classify the monomial Kummer subspaces of division cyclic algebras of prime degree  $p$ , showing that every such space is standard, and in particular the dimension is no greater than  $p + 1$ . It follows that in a generic cyclic algebra, the dimension of any Kummer subspace is at most  $p + 1$ .

**Keywords:** Central Simple Algebras, Cyclic Algebras, Kummer Spaces, Generic Algebras, Zero Sum Sequences

**2010 MSC:** Primary 16K20; Secondary 11J13

---

## 1. Introduction

Given an integer  $n$  and a central simple  $F$ -algebra  $A$  whose degree is a multiple of  $n$ , an  $n$ -Kummer element is an element  $v \in A$  satisfying  $v^n \in F^\times$  and  $v^{n'} \notin F$  for any  $1 \leq n' < n$ . (We omit  $n$  when it is obvious from the context.) These elements play an important role in the structure and presentations of these algebras. For

---

*Email addresses:* adam1chapman@yahoo.com (Adam Chapman), diambri@hotmail.com (David J. Gryniewicz), elimatzri@gmail.com (Eliyahu Matzri), rowen@math.biu.ac.il (Louis H. Rowen), vishne@math.biu.ac.il (Uzi Vishne)

example, in case  $\deg(A) = n$  and  $F$  is a field of characteristic prime to  $n$  containing a primitive  $n$ th root of unity,  $A$  is cyclic if and only if it contains a Kummer element. Without roots of unity, this equivalence holds when  $n$  is prime, but there are counterexamples for general  $n$ . (See [MRV12].)

A Kummer subspace of  $A$  is an  $F$ -vector subspace  $V$  where every  $v \in V \setminus \{0\}$  is Kummer. In case  $F$  is of characteristic prime to  $n$  containing a primitive  $n$ th root of unity  $\rho$ , every cyclic algebra of degree  $n$  over  $F$  can be presented as

$$F[x, y \mid x^n = \alpha, y^n = \beta, yxy^{-1} = \rho x]$$

for some  $\alpha, \beta \in F^\times$ . Assume  $A$  is a tensor product of  $m$  cyclic algebras of degree  $n$  over  $F$ , and fix a presentation

$$A = \bigotimes_{k=1}^m F[x_k, y_k : x_k^n = \alpha_k, y_k^n = \beta_k, y_k x_k y_k^{-1} = \rho x_k].$$

**Definition 1.1.** *A monomial Kummer subspace of  $A$  (with respect to that fixed presentation) is a Kummer space spanned by elements of the form  $\prod_{k=1}^m x_k^{a_k} y_k^{b_k}$  for some  $0 \leq a_1, b_1, \dots, a_m, b_m \leq n - 1$ .*

Assume from now on that  $n = p$  is prime. In [Mat], the author made use of the existence of  $(mp + 1)$ -dimensional monomial Kummer spaces in  $A$  to prove that the symbol length of any central simple  $F$ -algebras is bounded from above by  $p^{r-1} - 1$  when  $F$  is a  $C_r$  field. We are interested therefore in the maximal possible dimension of Kummer spaces in general, and monomial Kummer spaces in particular. Another motivation comes from the generalized Clifford algebras: if  $p + 1$  is indeed the maximal dimension of a Kummer space in a cyclic algebra of degree  $p$ , as we conjecture, then the Clifford algebra of a nondegenerate homogeneous polynomial form of degree  $p$  in more than  $p + 1$  variables cannot have simple images of degree  $p$ . (See [CV12] for more information on generalized Clifford algebras.)

In tensor products of  $m$  quaternion algebras, the dimension of Kummer spaces is bounded by  $2m + 1$ . This is an immediate result of the theory of Clifford algebras of quadratic forms. (See [Lam73] for further information.) The Kummer subspaces of cyclic algebras of degree 3 were classified in [Rac09], and then in [MV12] and [MV14], using techniques of composition algebras suggested by J.-P. Tignol. The monomial Kummer subspaces of the tensor product of  $m$  cyclic algebras of degree 3 were classified in [Cha], establishing an upper bound of  $3m + 1$ . This upper bound holds also for non-monomial Kummer spaces in the generic tensor product of  $m$  cyclic algebras.

In this paper we study Kummer subspaces in cyclic algebras of degree  $p$  for any prime  $p$ . We prove that the dimension of monomial Kummer spaces in such algebras is bounded by  $p + 1$ . The proof of this algebraic fact requires a nontrivial result from elementary number theory ([LPYZ10], see also [GV]). Finally, we prove in Section 4 that  $p + 1$  is the upper bound for the dimension of any Kummer subspace in the generic cyclic algebra.

## 2. Kummer subspaces

Let  $p$  be a prime number,  $F$  be a field of characteristic either 0 or greater than  $p$  containing a primitive  $p$ th root of unity  $\rho$ , and  $A$  be a cyclic division algebra of degree  $p$  over  $F$ . The variety  $X_A$  of all Kummer elements in  $A$  is defined by the condition  $s_1 = \cdots = s_{p-1} = 0$ , where  $s_i$  are the generic characteristic coefficients. We assume that  $p \geq 5$ .

### 2.1. Standard Kummer subspaces

Let  $x \in X_A$ . For any  $1 \leq k \leq p - 1$  we set

$$V_k(x) = Fx + \{w \in A : wx = \rho^k xw\}.$$

**Proposition 2.1.** *Fix  $k$ .*

1. *For every  $x \in X_A$ ,  $V_k(x)$  is a Kummer space.*
2. *The Kummer space  $V_k(x)$  determines  $x$  up to a scalar factor.*

*Proof.* Let  $x \in X_A$ . By the Skolem-Noether Theorem, there is a Kummer element  $y$  such that  $xyx^{-1} = \rho x$ , and then  $V_k(x) = Fx + F[x]y^k$ . For every  $c \in F[x]$ ,  $(x + cy^k)^p = x^p + N_{F[x]/F}(c)y^{kp} \in F$ , proving that  $Fx + F[x]y^k$  is a Kummer space.

Suppose  $V_1(x) = V_1(x')$  for  $x, x' \in X_A$ . As before let  $y, y' \in X_A$  be elements such that  $xyx^{-1} = \rho x$  and  $y'x'y'^{-1} = \rho x'$ . Let  $\sigma$  denote the automorphism of  $F[x]$  induced by conjugation by  $y$ . Since  $x', y' \in V_k(x)$ , we can write  $x' = \alpha x + wy$  and  $y' = \beta x + w'y$  for  $\alpha, \beta \in F$  and  $w, w' \in F[x]$ . The condition  $y'x' = \rho x'y'$  gives

$$\begin{aligned} \alpha\beta x^2 + (\beta xw + \rho\alpha xw')y + w'\sigma(w)y^2 \\ = \rho\alpha\beta x^2 + (\rho^2\beta xw + \rho\alpha xw')y + \rho w\sigma(w')y^2, \end{aligned} \tag{1}$$

which implies  $\alpha\beta = 0$ . If  $\beta \neq 0$  then  $\alpha = 0$  implies  $w = 0$ , which is impossible. Therefore  $\beta = 0$ , and the remaining equation is

$$w'\sigma(w) = \rho w\sigma(w'),$$

from which it follows that  $w \in Fxw'$ . But since  $x'y' \in V_1(x') = V_1(x)$ , the coefficient of  $y^2$  in  $x'y'$  must be zero, and hence  $w\sigma(w') = 0$ . However  $w' \neq 0$ , and therefore  $x' \in Fx$ .

The general argument is obtained by replacing  $\rho$  with  $\rho^k$ .  $\square$

**Definition 2.2.** A Kummer subspace  $V \subseteq A$  is called **standard** if it is contained in a space of the form  $V_k(x)$  for some Kummer element  $x$  and  $0 \leq k \leq p-1$ .

## 2.2. Criteria for being Kummer

In order to simplify the expressions, we adopt the following symmetric product notation from [Rev77]: Given  $v_1, \dots, v_t \in A$ , let  $v_1^{i_1} * \dots * v_t^{i_t}$  denote the sum of the products of the elements  $v_1, \dots, v_1, v_2, \dots, v_2, \dots, v_t, \dots, v_t$  in all possible rearrangements, where each  $v_k$  appears exactly  $i_k$  times. The superscript  $i_k = 1$  is omitted, so for example  $x^1 * y^2 = x * y^2$ . The exponentiation notation is used strictly in this sense. We use parentheses when the symmetric product is applied to monomials. For instance,  $(x^3)^2 * (y^5) = x^6y^5 + x^3y^5x^3 + y^5x^6$ .

**Proposition 2.3.** Let  $v_1, \dots, v_t \in A$ . The subspace  $V = Fv_1 + \dots + Fv_t$  is Kummer if and only if

$$v_1^{i_1} * \dots * v_t^{i_t} \in F$$

for every  $i_1, \dots, i_t \geq 0$  with  $i_1 + \dots + i_t = p$ .

*Proof.* By definition  $V = Fv_1 + \dots + Fv_t$  is Kummer if and only if  $\lambda_1v_1 + \dots + \lambda_tv_t$  is Kummer for every  $\lambda_1, \dots, \lambda_t \in F$ , i.e.

$$\sum_{i_1, \dots, i_t} (v_1^{i_1} * \dots * v_t^{i_t}) \lambda_1^{i_1} \dots \lambda_t^{i_t} = (\lambda_1v_1 + \dots + \lambda_tv_t)^p \in F.$$

Since  $F$  is infinite, the latter is equivalent to having the coefficients  $v_1^{i_1} * \dots * v_t^{i_t}$  in  $F$ .  $\square$

**Remark 2.4.** Assume that  $Fv + Fv'$  is Kummer where  $v$  and  $v'$  commute. Then  $v$  and  $v'$  are linearly dependent.

Indeed,  $pv^{p-1}v' = v^{p-1} * v' \in F$ , so  $v^{-1}v' \in F$ .

**Theorem 2.5.** For every  $x \in X_A$  and  $k$ ,  $V_k(x)$  is maximal with respect to inclusion as a Kummer subspace.

*Proof.* The proof appears in a more general context in [Cha]. As before it suffices to prove that  $V_1(x)$  is maximal. Let  $y$  be an invertible element such that  $xyx^{-1} = \rho x$ , so that  $V = V_1(x) = Fx + F[x]y$ . Let  $z \in A$ , and assume  $V + Fz$  is Kummer; we need to show that  $z \in V$ . Write  $z = \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} \alpha_{a,b} x^a y^b$  for  $\alpha_{a,b} \in F$ . (We have  $\alpha_{0,0} = 0$  because  $\text{Tr}(z) = 0$ .) For every  $a, b$ , there exists some  $\ell \not\equiv 0 \pmod{p}$  such that  $x^{a\ell} y^{b\ell} \in V$ : If  $b \neq 0$  then take  $\ell \equiv b^{-1} \pmod{p}$ . Otherwise take  $\ell \equiv a^{-1} \pmod{p}$ . For any  $a$  and  $b$ ,

$$\begin{aligned} \sum_{ij} \alpha_{i,j} ((x^{a\ell} y^{b\ell})^{p-1} * (x^i y^j)) &= (x^{a\ell} y^{b\ell})^{p-1} * \sum_{ij} \alpha_{i,j} (x^i y^j) \\ &= (x^{a\ell} y^{b\ell})^{p-1} * z \in F. \end{aligned}$$

The coefficient of  $x^{a(1-\ell)} y^{b(1-\ell)}$  in this sum is

$$\alpha_{a,b} (x^{a\ell} y^{b\ell})^{p-1} * (x^a y^b) = p \alpha_{a,b} (x^{a\ell} y^{b\ell})^p = p (x^p)^{a\ell} (y^p)^{b\ell} \alpha_{a,b},$$

so if the monomial  $x^a y^b$  is not in  $V$ , then  $\ell \neq 1$  and necessarily  $\alpha_{a,b} = 0$ . Consequently  $z \in V$ .  $\square$

We conclude this section with another criterion for a subspace to be Kummer. We denote the reduced trace by  $\text{Tr}(\cdot)$ .

**Lemma 2.6.** *Let  $b_1, \dots, b_t \in A$ . The subspace  $V = Fb_1 + \dots + Fb_t$  is Kummer if and only if  $\text{Tr}(b_1^{i_1} * \dots * b_t^{i_t}) = 0$  for every  $i_1, \dots, i_t \geq 0$  satisfying  $i_1 + \dots + i_t < p$ .*

*Proof.* An element  $x \in A$  is Kummer if and only if  $\text{Tr}(x^i) = 0$  for every  $i = 1, \dots, p-1$ . The rest of the proof is the same as in Proposition 2.3.  $\square$

The usefulness of the second criterion is emphasized in the following observation:

**Lemma 2.7.** *Fix a presentation  $A = F[x, y \mid x^p = \alpha, y^p = \beta, yxy^{-1} = \rho x]$ . Let  $v_1, \dots, v_t$  be monomials. Then, for every  $i_1, \dots, i_t \geq 0$  with  $i_1 + \dots + i_t < p$ ,  $v_1^{i_1} * \dots * v_t^{i_t}$  is a nonzero multiple of  $v_1^{i_1} \dots v_t^{i_t}$ .*

*Proof.* Since each  $v_i$  is monomial, the multiplicative commutator of every  $v_j, v_{j'}$  is a power of  $\rho$ . Therefore, each summand in the symmetric product  $v_1^{i_1} * \dots * v_t^{i_t}$  is a multiple of  $v_1^{i_1} \dots v_t^{i_t}$  by some power of  $\rho$ , and when we write

$$v_1^{i_1} * \dots * v_t^{i_t} = c \cdot v_1^{i_1} \dots v_t^{i_t},$$

we have that  $c \in \mathbb{Z}[\rho]$  (more precisely in the image of  $\mathbb{Z}[\rho]$  in  $F$ ).

Modulo  $1 - \rho$ ,  $c$  is equivalent to the number of summands, namely  $c \equiv \binom{i_1 + \dots + i_t}{i_1, \dots, i_t}$  in the quotient  $\mathbb{Z}[\rho]/(1 - \rho)\mathbb{Z}[\rho] \cong \mathbb{Z}/p\mathbb{Z}$ . But the multinomial coefficient is nonzero modulo  $p$  because  $(i_1 + \dots + i_t)!$  is prime to  $p$ .  $\square$

### 3. Monomial Kummer subspaces

Fix a presentation

$$A = F[x, y \mid x^p = \alpha, y^p = \beta, yxy^{-1} = \rho x].$$

Recall that a Kummer subspace  $V \subseteq A$  is **monomial** if it is spanned by elements of the form  $x^i y^j$ . In this section we classify monomial Kummer subspaces, showing that they are all standard.

**Lemma 3.1.** *A subspace  $V \subseteq A$  is monomial if and only if it is invariant under conjugation by  $x$  and  $y$ .*

*Proof.* A monomial subspace is obviously invariant. Assume  $V$  is invariant under conjugation by  $x$  and  $y$ . Let  $v \in A$ . Write

$$v = f_0 + f_1 y + \cdots + f_{p-1} y^{p-1}$$

where  $f_0, \dots, f_{p-1} \in F[x]$ . Then

$$\sum_{i=0}^{p-1} \rho^{-ij} f_i y^i = x^j v x^{-j} \in V$$

for  $0 \leq j < p$ , implying by a standard Vandermonde argument (based on the fact that the matrix  $(\rho^{ij}) : 0 \leq i, j < p$  is invertible) that  $f_i y^i \in V$  for each  $0 \leq i \leq p-1$ . Now writing  $f_i = \sum_j \alpha_{i,j} x^j$  for  $\alpha_{i,j} \in F$  and conjugating by  $y$  yields by the same argument that each  $\alpha_{i,j} x^j y^i \in V$ . Going over all the elements in  $V$ , one obtains a set of monomials in  $V$  spanning  $V$ .  $\square$

#### 3.1. 3-dimensional Kummer spaces

We commence with Kummer spaces of dimension 3.

**Remark 3.2.** *In the following cases, the space*

$$U = Fx + Fy + Fx^a y^b$$

*is Kummer:  $a = 1, b = 1, a + b \equiv 0 \pmod{p}$  and  $a + b \equiv 1 \pmod{p}$ . In all of these cases  $U$  is standard:*

$$\begin{aligned} Fx + Fy + Fxy^b &\subseteq Fy + F[y]x; \\ Fx + Fy + Fx^a y &\subseteq Fx + F[x]y; \\ Fx + Fy + Fx^a y^{-a} &\subseteq F(xy^{-1})^a + F[xy^{-1}]y; \\ Fx + Fy + Fx^a y^{1-a} &\subseteq F[xy^{-1}]y. \end{aligned}$$

For every integer  $a \in \mathbb{Z}$ , let  $(a)_p$  denote the unique residue  $(a)_p \equiv a \pmod{p}$  such that  $0 \leq (a)_p < p$ .

**Proposition 3.3.** *Let  $U = Fx + Fy + Fx^a y^b$ . Then  $U$  is not Kummer if and only if there is some  $k$ , invertible modulo  $p$ , such that  $(ka)_p + (kb)_p + (-k)_p < p$ .*

*Proof.* For every positive  $i, j, k$  with  $i+j+k < p$ , write  $x^i * y^j * (x^a y^b)^k = c_{ijk} x^{i+ka} y^{j+kb}$  for a suitable constant  $c_{ijk} \in \mathbb{Z}[\rho]$ , which is nonzero by Lemma 2.7.

By Lemma 2.6,  $U$  is not Kummer if and only if there are some positive  $i, j, k$  with  $i + j + k < p$  such that

$$c_{ijk} \text{Tr}(x^{i+ka} y^{j+kb}) = \text{Tr}(x^i * y^j * (x^a y^b)^k) \neq 0.$$

But the reduced trace of a non-central monomial is zero, so  $U$  is not Kummer if and only if there are positive  $i, j, k$  with  $i + j + k < p$  for which  $x^{i+ka} y^{j+kb} \in F$ , namely  $i \equiv -ka$ ,  $j \equiv -kb$ .  $\square$

Let  $\langle z \rangle$  denote  $F^\times z$  for any  $z \in X_A$ . Consider the subgroup  $G$  of  $A^\times / F^\times$  generated by  $F^\times x$  and  $F^\times y$ . Clearly  $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ .

**Proposition 3.4.** *Given  $z_1, z_2, z_3 \in X_A$ , the space*

$$U = Fz_1 + Fz_2 + Fz_3$$

*is Kummer if and only if:*

1. *there are no  $i \neq j$  with  $z_j \in \langle z_i \rangle$ , and*
2. *either  $\langle z_i z_j^{-1} \rangle = \langle z_k \rangle$  for some permutation  $\{i, j, k\}$  of  $\{1, 2, 3\}$ , or  $\langle z_1 z_2^{-1} \rangle = \langle z_2 z_3^{-1} \rangle = \langle z_3 z_1^{-1} \rangle$ .*

*Proof.* The first requirement follows from Proposition 2.4. Therefore, we may assume that any two of  $\langle z_1 \rangle, \langle z_2 \rangle, \langle z_3 \rangle$  generate  $G$ . By changing generators and the choice of root of unity, we may assume  $z_1 = x$  and  $z_2 = y$ . The condition then translates to:  $U = Fx + Fy + Fx^a y^b$  is Kummer if and only if one of the following holds:

1.  $\langle xy^{-1} \rangle = \langle x^a y^b \rangle$ , or equivalently,  $a + b \equiv 0 \pmod{p}$ ;
2.  $\langle y \rangle = \langle x^{a-1} y^b \rangle$ , or equivalently,  $a = 1$ ;
3.  $\langle x \rangle = \langle x^a y^{b-1} \rangle$ , or equivalently,  $b = 1$ ;
4.  $\langle xy^{-1} \rangle = \langle x^{a-1} y^b \rangle = \langle x^a y^{b-1} \rangle$ , or equivalently,  $a + b \equiv 1 \pmod{p}$ .

These are the cases listed in Remark 3.2 as Kummer subspaces, and it remains to show that  $U$  is not Kummer in any other case. Let  $a, b \in \mathbb{Z}/p\mathbb{Z}$  be numbers such that  $x^a y^b$  is not in  $\langle x \rangle$  or  $\langle y \rangle$ , and such that we are not in any of the four cases listed above. Consider the vector  $(a, b, -1)$  over  $\mathbb{Z}/p\mathbb{Z}$ . It has no zero entries, no sum of two entries is zero, and  $a + b - 1$  is nonzero. It was shown in [LPYZ10] that there is some invertible  $k \in \mathbb{Z}/p\mathbb{Z}$  such that  $(ak)_p + (bk)_p + (-k)_p < p$ , so  $U$  is not Kummer by Proposition 3.3.  $\square$

### 3.2. Kummer spaces of dimension greater than 3

**Lemma 3.5.** *The space  $U = Fx + Fy + Fx^a y^b + Fx^c y^d$  is not Kummer if there are integers  $m, \ell$  such that  $0 < (am + c\ell)_p + (bm + d\ell)_p + (-m)_p + (-\ell)_p < p$ .*

*Proof.* Assume such integers exist. Then  $w = x^{(am+c\ell)_p} y^{(bm+d\ell)_p} (x^a y^b)^{(-m)_p} (x^c y^d)^{(-\ell)_p}$  is a nonzero multiple of the scalar  $x^{(am+c\ell)_p} y^{(bm+d\ell)_p} (x^a y^b)^{(-m)_p} (x^c y^d)^{(-\ell)_p}$  by Lemma 2.7, so that  $\text{Tr}(w) \neq 0$ , and Lemma 2.6 shows that  $U$  is not Kummer.  $\square$

**Theorem 3.6.** *Every monomial Kummer space of dimension greater than 3 whose basis contains  $x$  and  $y$  is contained in either*

- $V_1(x) = F[x]y + Fx$ , or
- $V_{p-1}(y) = F[y]x + Fy$ , or
- $V_k(v) = F[v]x + Fv$  where  $v = (xy^{-1})^k$  for some  $1 \leq k \leq p-1$ .

*Proof.* Let  $\{x, y, u, w, \dots\}$  be the basis. Assume  $u = xy^k$  and  $w = x^i y$  for some  $1 \leq k, i \leq p-1$ . Since  $\langle w \rangle = \langle u^{k^{-1}} x^{i-k^{-1}} \rangle$ , one of the following holds:  $k = 1$ ,  $i - k^{-1} \equiv 1 \pmod{p}$ ,  $k^{-1} + i - k^{-1} = i \equiv 0 \pmod{p}$  or  $i \equiv 1 \pmod{p}$ . The case of  $i \equiv 0$  is out of the question. If  $i, k \neq 1$  then  $i - k^{-1} \equiv 1 \pmod{p}$ , which means that  $ki - 1 \equiv k \pmod{p}$ . For similar reasons we obtain from  $\langle u \rangle = \langle w^{i^{-1}} y^{k-i^{-1}} \rangle$  that  $ki - 1 \equiv i \pmod{p}$ . Therefore,  $k = i$ . However, in this case the condition from Lemma 3.5 for not being Kummer holds for this space: take  $m = -1$  and  $\ell = 2i - 2$  if  $i \leq \frac{p-1}{2}$ , and  $m = -1$  and  $\ell = -1$  if  $\frac{p+1}{2} \leq i$ .

Assume  $u = x^i y$  and  $w = x^{-k} y^k$  for some  $1 \leq k, i \leq p-1$ . Since  $\langle w \rangle = \langle u^k x^{-k-ik} \rangle$ , either  $k = 1$ ,  $-k - ik \equiv 1 \pmod{p}$ ,  $k - k - ik = -ik \equiv 0 \pmod{p}$  or  $-ik \equiv 1 \pmod{p}$ . In case  $k = 1$ ,  $w, u \in F[x]y$ . Assume  $k \neq 1$ . The case of  $-ik \equiv 0 \pmod{p}$  is impossible. From  $\langle w \rangle = \langle u^{-ki^{-1}} y^{k+ki^{-1}} \rangle$  we obtain that either  $-ki^{-1} \equiv 1 \pmod{p}$ ,  $k + ki^{-1} \equiv 1 \pmod{p}$ ,  $k = 0$  or  $k = 1$ . The two last options are out of the question. The first option implies  $i \equiv -k \pmod{p}$  and the



second  $ki + k \equiv i \pmod{p}$ . If  $i \equiv -k \pmod{p}$  and  $-ik \equiv 1 \pmod{p}$  then  $k^2 \equiv 1 \pmod{p}$  which means  $k = p - 1$ . In this case,  $w, u \in F[y]x$ . If  $i \equiv -k \pmod{p}$  and  $-k - ik \equiv 1 \pmod{p}$  then  $k^2 - k - 1 \equiv 0 \pmod{p}$ . However, in this case the condition from Lemma 3.5 for not being Kummer holds for this space: take  $m = -1$  and  $\ell = k + 1$  if  $\frac{p+1}{2} \leq k$ , and  $m = 2 - k$  and  $\ell = -1$  if  $k \leq \frac{p-1}{2}$ . If  $ki + k \equiv i \pmod{p}$  and  $-k - ik \equiv 1 \pmod{p}$  then  $i = p - 1$ . In this case,  $w$  commutes with  $v$ , contradiction. If  $ki + k \equiv i \pmod{p}$  and  $-ik \equiv 1 \pmod{p}$  then  $k \equiv i + 1 \pmod{p}$ . In this case, the condition from Lemma 3.5 for not being Kummer holds for this space: take  $m = \ell = -1$ .

Assume  $u = x^i y$  and  $x^{-k} y^{k+1}$  for some  $1 \leq i \leq p - 1$  and  $1 \leq k \leq p - 2$ . Since  $\langle w \rangle = \langle u^{k+1} x^{-k-i(k+1)} \rangle$ , either  $k = 0$ ,  $-k - i(k+1) \equiv 1 \pmod{p}$ ,  $1 - i(k+1) \equiv 0 \pmod{p}$  or  $-i(k+1) \equiv 0 \pmod{p}$ . The first option is impossible. The last option implies  $k = p - 1$ , contradiction. From  $\langle w \rangle = \langle u^{-ki^{-1}} y^{k+1+ki^{-1}} \rangle$ , either  $-ki^{-1} \equiv 1 \pmod{p}$ ,  $k + 1 + ki^{-1} \equiv 1 \pmod{p}$ ,  $k = p - 1$  or  $k = 0$ . The last two options are impossible. The first option translates to  $i \equiv -k \pmod{p}$  and the second to  $k(i+1) \equiv 0 \pmod{p}$ , i.e.  $i = p - 1$ . If  $i = p - 1$  then  $w, u \in F[u]x + Fu$ . Assume  $i \equiv -k \pmod{p}$  and  $i \neq p - 1$ . If  $-k - i(k+1) \equiv 1 \pmod{p}$  then  $k^2 \equiv 1 \pmod{p}$ , which means  $k = p - 1$  or  $k = 1$ , contradiction. If  $1 - i(k+1) \equiv 0 \pmod{p}$  then  $k^2 + k + 1 \equiv 0 \pmod{p}$ . In this case, however, the condition from Lemma 3.5 for not being Kummer holds for this space: take  $m = -1$  and  $\ell = 2 + k$ .

If  $u = x^{-k} y^k$  and  $w = x^{-i} y^i$  then  $u$  and  $w$  commute, contradiction. If  $u = x^{-k} y^k$  and  $w = x^{-i} y^{i+1}$  then  $w, u \in F[u]w + Fu$ .

In conclusion, if the basis contains a monomial of the form  $x^i y$  with  $2 \leq i \leq p - 2$  then all the other basic elements must belong to  $F[x]y$ . Similarly, if the basis contains a monomial of the form  $xy^k$  with  $2 \leq k \leq p - 2$  then all the other basic elements must belong to  $F[y]x$ . If the basis contains a monomial of the form  $x^{-k} y^k$  with  $2 \leq k \leq p - 2$  then all the other basic elements must belong to  $F[x^{-k} y^k]x + x^{-k} y^k$ . If the basis contains the monomial  $xy$  then all the other basic elements must belong to  $F[x]y + F[y]x$ . If the basis contains the monomial  $x^{p-1} y$  then all the other basic elements belong to  $F[x]y + F[x^{-1} y]x$ . If the basis contains the monomial  $xy^{p-1}$  then all the other basic elements belong to  $F[y]x + F[x^{-1} y]x$ . The monomial Kummer spaces that do not contain elements of the forms  $x^i y$ ,  $xy^k$ ,  $x^{-k} y^k$  are contained in  $F[x^{-1} y]x$ . The statement follows immediately.  $\square$

All the arguments in this section can be repeated for any pair of monomials in the basis of a monomial Kummer space, not just  $x$  and  $y$ . Therefore we obtain the following:

**Corollary 3.7.** *Every monomial Kummer space is standard. In particular, the dimension of any monomial Kummer space is at most  $p + 1$ .*

#### 4. Kummer subspaces in the generic cyclic algebra of degree $p$

In this section we consider maximal Kummer subspaces in the generic cyclic algebra of degree  $p$ , and show that their dimension is at most  $p + 1$ .

The generic cyclic algebra is constructed as follows, when the ground field  $F$  has characteristic prime to  $p$  and contains  $p$ th roots of unity: Let

$$T = F[X, Y : YX = \rho XY]$$

denote the quantum plane with the commutator specialized to  $\rho$ . Let  $\alpha = X^p$  and  $\beta = Y^p$ . Localizing at the center  $T_0 = F[X^p, Y^p]$ , we obtain the division algebra  $D = (T_0 \setminus \{0\})^{-1}T$ , which is cyclic over its own center  $K = q(T_0) = F(\alpha, \beta)$ . This algebra is generic as a cyclic algebra, as we can specialize  $X, Y$  to a standard pair of generators in any cyclic division algebra over  $F$ .

Every element of  $T$  can be written uniquely as a polynomial of the form  $\sum_{i,j=0}^N \alpha_{ij} X^i Y^j$  with coefficients  $\alpha_{ij} \in F$ . This induces a natural  $\mathbb{Z} \times \mathbb{Z}$ -grading where the homogeneous components are monomials in  $X, Y$  over  $F$ . We order  $\mathbb{Z} \times \mathbb{Z}$  lexicographically and denote by  $\deg(t)$  the degree of  $t$ , and by  $\text{top}(t)$  the leading monomial of  $t \in T$ , namely when  $t = \sum a_{i,j} X^i Y^j$ ,  $\deg(t) = (i, j)$  and  $\text{top}(t) = a_{i,j} X^i Y^j$  with  $(i, j)$  maximal such that  $a_{i,j} \neq 0$ .

**Remark 4.1.** *For every  $t_1, t_2 \in T$ ,  $\text{top}(t_1 t_2) = \text{top}(t_1) \text{top}(t_2)$ .*

Now let  $V \subseteq D$  be a Kummer subspace. Clearing denominators in a basis of  $V$  over the center, we may write  $V = K \cdot V_0$  where  $V_0 \subseteq T$  is a (finite) module over  $T_0$ .

**Proposition 4.2.** *Let  $v_1, \dots, v_k \in T$ . If  $V = Fv_1 + \dots + Fv_k \subset D$  is Kummer then so is  $\hat{V} = F \text{top}(v_1) + \dots + F \text{top}(v_k)$ .*

*Proof.* By Lemma 2.6, we only need to show that  $\text{Tr}(\text{top}(v_1)^{i_1} \cdots \text{top}(v_k)^{i_k}) = 0$  for every  $i_1, \dots, i_k \geq 0$  with  $i_1 + \dots + i_k < p$ . Since  $\text{top}(v_1)^{i_1} \cdots \text{top}(v_k)^{i_k}$  is a multiple of  $\text{top}(v_1)^{i_1} \cdots \text{top}(v_k)^{i_k}$ , we need only show that  $\text{Tr}(\text{top}(v_1)^{i_1} \cdots \text{top}(v_k)^{i_k}) = 0$ .

But the fact that  $V$  is Kummer implies  $\text{Tr}(v_1^{i_1} \cdots v_k^{i_k}) = 0$ , which in particular implies that its coefficient of degree  $i_1 \deg(v_1) + \dots + i_k \deg(v_k)$  is zero. This coefficient is  $\text{Tr}(\text{top}(v_1)^{i_1} \cdots \text{top}(v_k)^{i_k})$ , a nonzero multiple of  $\text{Tr}(\text{top}(v_1)^{i_1} \cdots \text{top}(v_k)^{i_k})$ , by Lemma 2.7, so  $\text{Tr}(\text{top}(v_1)^{i_1} \cdots \text{top}(v_k)^{i_k}) = 0$  as desired.  $\square$

**Remark 4.3.** *A Kummer subspace  $V \subset D$  has a basis contained in  $T$  and with distinct degrees modulo  $p\mathbb{Z} \times p\mathbb{Z}$ .*

*Proof.* Clearing denominators we may assume the basis elements  $v_1, \dots, v_k$  are in  $T$ . Fix an arbitrary linear order on  $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ . The degree of  $v \in T$  now denotes the maximal  $(i, j)$  for which  $v$  has a monomial in  $F[\alpha, \beta]X^iY^j$ . If some  $v_r, v_s$  ( $r < s$ ) have the same degree, let  $c_r$  and  $c_s$  denote the coefficients of the leading monomials, and replace  $v_s$  by  $c_r v_s - c_s v_r$ . This does not change  $\sum K v_i$ . Moreover the resulting vector cannot be zero because of the independence over  $K$ . And finally the degree vector of  $v_1, \dots, v_k$  has been lexicographically reduced, establishing that the process is finite, culminating in the desired basis.  $\square$

**Theorem 4.4.** *The dimension of a Kummer subspace of  $D$  is at most  $p + 1$ .*

*Proof.* Let  $V \subseteq D$  be a Kummer subspace. By Remark 4.3 there is a basis  $v_1, \dots, v_k$  of  $V$  whose elements are in  $T$  and have distinct degrees modulo  $p\mathbb{Z} \times p\mathbb{Z}$ . The space  $\hat{V} = F \text{top}(v_1) + \dots + F \text{top}(v_k)$  is clearly monomial (with respect to  $X, Y$ ) and is Kummer by Proposition 4.2. By Corollary 3.7,  $\dim(V) = \dim(\hat{V}) \leq p + 1$ .  $\square$

## Acknowledgements

This work is the outcome of the noncommutative algebra group meetings held at Bar-Ilan University during the academic year 2012-2013. Chapman, Rowen and Vishne were partially supported by BSF grant 2010/149. Gryniewicz was partially supported by FWF grant P21576-N18. Matzri was partially supported by a Kreitman fellowship and by the Israel Science Foundation (grant No. 152/13).

## Bibliography

### References

- [Cha] Adam Chapman, *Kummer subspaces of tensor products of cyclic algebras*, arXiv:1405.0188v1.
- [CV12] Adam Chapman and Uzi Vishne, *Clifford algebras of binary homogeneous forms*, J. Algebra **366** (2012), 94–111. MR 2942645
- [GV] David J. Gryniewicz and Uzi Vishne, *Projective norms modulo  $n$* , in preparation.

- [Lam73] T. Y. Lam, *The algebraic theory of quadratic forms*, W. A. Benjamin, Inc., Reading, Mass., 1973, Mathematics Lecture Note Series. MR 0396410 (53 #277)
- [LPYZ10] Y. Li, C. Plyley, P. Yuan, and X. Zeng, *Minimal zero sum sequences of length four over finite cyclic groups*, J. Number Theory **130** (2010), 2033–2048.
- [Mat] Eliyah Matzri, *Symbol length in the brauer group of a field*, to appear in Trans. Amer. Math. Soc.
- [MRV12] Eliyahu Matzri, Louis H. Rowen, and Uzi Vishne, *Non-cyclic algebras with  $n$ -central elements*, Proc. Amer. Math. Soc. **140** (2012), no. 2, 513–518. MR 2846319 (2012i:16034)
- [MV12] Eliyahu Matzri and Uzi Vishne, *Isotropic subspaces in symmetric composition algebras and Kummer subspaces in central simple algebras of degree 3*, Manuscripta Math. **137** (2012), no. 3-4, 497–523. MR 2875290
- [MV14] ———, *Composition algebras and cyclic  $p$ -algebras in characteristic 3*, Manuscripta Math. **143** (2014), no. 1-2, 1–18. MR 3147442
- [Rac09] Mélanie Raczek, *On ternary cubic forms that determine central simple algebras of degree 3*, J. Algebra **322** (2009), no. 5, 1803–1818. MR 2543635 (2010h:16043)
- [Rev77] Ph. Revoy, *Algèbres de Clifford et algèbres extérieures*, J. Algebra **46** (1977), no. 1, 268–277. MR 0472881 (57 #12568)